The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.16
The USAP Certification & Accreditation Program

Organizational Function	Information Resource Management	Policy Number	5000.16
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Updated	24 April 2007
Subject	Certification & Accreditation Program	Authorized By	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Antarctic Infrastructure & Logistics	Responsible Official	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone	703.292.8032
		Fax	703.292.9080
		Web	www.nsf.gov
Distribution	USAP-Wide	Status	Final Policy
Online Publication	www.usap.gov		

1. PURPOSE

This directive establishes the Certification and Accreditation (C&A) program for information systems supporting the National Science Foundation (NSF) Office of Polar Programs (OPP), United States Antarctic Program (USAP). This directive establishes quality controls for the security of information resources. Certification is the technical evaluation of the risks associated with system operations. Accreditation is the management acceptance of the evaluated risk factors and the resulting approval or denial to operate the system. The Certification and Accreditation program applies to all applications and systems that are determined to be Major Applications or General Support Systems, as defined by the Federal Information Security Management Act of 2002 (FISMA). The USAP Certification and Accreditation program includes activities to support the implementation of NSF FISMA directives.

2. BACKGROUND

Federal information technology regulations require USAP information systems to undergo a security certification and accreditation process to identify the risks associated with their operation. USAP information system integrity ensures the success of the science research mission by providing reliable global communications to facilitate field experiments and exchange of data within the Antarctic region. It also protects government and private resources used to execute and administer mission activities while allowing effective access to program information by the general public.

3. GUIDING PRINCIPLES

- The USAP C&A process will be an integral element of information systems development and operation.
- The USAP C&A process is based on existing federal and NSF directives, particularly those listed in 5000.1, Appendix 1.
- Science grant systems will be included in the Certification & Accreditation process as directed by NSF OPP

4. POLICY

The C&A process will implement the policies of the NSF and the National Institute of Standards and Technology (NIST) as they apply to the USAP.

4.1 Operational Definitions

4.1.1 Accreditation

A formal declaration by the Designated Approving Authority (DAA), that an information system is approved for operation, employing the safeguards documented in the system Certification. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security during the development of the system.

4.1.2 Certification

The technical evaluation of an information system's security features and other safeguards that establish the extent to which they meet security requirements to withstand identified threats at evaluated levels of risk and probability.

4.1.3 Designated Approving Authority (DAA)

Per NSF Manual 7, The NSF Information Security Handbook, the Designated Approving Authority for USAP systems is the NSF CIO.

4.1.4 General Support System

As defined in Circular A-130, Appendix III, a General Support System is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. Examples of a system are: a local area network (LAN) including smart terminals that supports a branch office; an agency-wide backbone; a communications network; a departmental data processing center including its operating system and utilities; a tactical radio network; and a shared information processing service organization.

4.1.5 Major Application

Is defined in Circular A-130 as an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

4.2 Certification and Accreditation Program (C&A)

The USAP Information Security Manger (ISM) will establish a program to certify and accredit the NSF-funded information systems used within the program. The program will include a process for certifying and accrediting systems, and procedures to guide information system managers through the process. Personal use systems are not normally included in the certification process, unless identified as part of a science grant system requiring certification review.

4.3 Identification of Included Information Systems

All Information and Information Technology, applications and systems determined to be either Major Applications or General Support Systems (hardware, software, information, data, applications, communications, and people) must complete the C&A process. Using the guidelines in Manual 7, the ISM will establish and maintain a list of major applications and general support systems at each USAP operating location. The list will be updated annually, or when major changes occur. Copies will be submitted to NSF/OPP to comply with NSF policies. The list will be included in the USAP Information Security Plan.

4.4 Participation

All USAP organizational elements, U.S. Government employees, research grantees, private citizens, contractors and sub-contractors personnel, and foreign nationals will support the C&A program in an appropriate manner.

4.5 Site Certification and Accreditation

The USAP Information Security Manager (ISM), with support from the USAP prime contractor will create a site certification package for each USAP operating location. The package will contain the same elements required for system certification by NIST guidelines. The package will be reviewed every year, to comply with NSF and FISMA requirements. The package will be updated every three years, or after major changes occur at the locations.

4.6 New Information Systems

To comply with OMB Circular A-130, all new information systems acquired or developed by any USAP participant organization to support program requirements will incorporate provisions for security certification and accreditation in their project and system life cycle planning. All new systems acquired or developed by any USAP participant organization will be checked against the criteria for major applications or general support systems provided by NSF/CIO. If the new information system is determined to be a major application or a general support system, the project to acquire the system will include funding in the system development plans to accomplish the system certification and accreditation.

4.7 Commercial Off-The-Shelf Applications

Commercial off-the-shelf (COTS) applications are covered by the C&A activities for the general support system on which they reside, unless the COTS product is identified as a major application.

4.8 Existing & Outdated Information Systems

Some USAP information systems that play a critical role in mission accomplishment entered into operation prior to implementation of this policy and have exceeded their design life. Where replacement systems have been identified and are under development, the C&A process will focus on the replacement system. Where no replacement has been identified, the C&A process will evaluate the existing system. NSF OPP will make the final determination as to whether or not a system requires certification and accreditation.

4.9 Periodic Review Of Information Systems

Federal guidelines direct that NSF perform an independent review or audit of the security controls in each major application or general support system at least every three years, or with a major change and based on these results, perform an annual review of the overall NSF-wide information security program. These periodic reviews, also include the USAP operating locations. At the start of each fiscal year, the USAP Information Security Manager will identify the systems to be reviewed in that fiscal year. This information will be included in the USAP Information Security Plan.

4.10 Federal Information Security Management Act of 2002 (FISMA)

The USAP certification and accreditation program includes responsibility for activities to comply with the Federal Information Security Management Act of 2002 (FISMA), which is the follow-on legislation to the Government Information Security Reform Act of 2000 (GISRA). Where possible, the C&A program will integrate FISMA/GISRA requirements into its overall structure. Any FISMA/GISRA requirements not integrated will still be managed under the C&A program.

4.11 Non-USAP Systems

Any Non-USAP system connected to the USAP information infrastructure must be evaluated to determine if a certification is required as part of the connection arrangements. NSF OPP makes the final determination as to whether or non a Non-USAP system requires a certification review as part of the connection arrangement.

4.12 Non-USAP Sites and Facilities

A non-USAP site or facility supports the USAP mission in some form, but is outside the direct management responsibility of the NSF. An example is a commercial satellite facility relaying information from a USAP operating location to the Denver HQs facility. This policy applies to non-USAP locations only to the extent required by federal law, or the grant, contract or other operating agreement in place between NSF and the party responsible for the non-USAP location.

5. APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this policy is as indicated in USAP Information Security Policy 5000.1, *The USAP Information Security Program*.

6. RESPONSIBILITIES

6.1 NSF Director of Polar Programs

The NSF Director of Polar Programs is the senior government executive responsible for USAP information systems, and is the USAP Certifying Official. The Certifying Official ensures that any security deficiencies are documented in the C&A Package. The Certifying Official determines the level of acceptable risk associated with system operation and recommends for or against accreditation to the NSF CIO, who is the Designated Accreditation Authority (DAA).

6.2 NSF Polar Research Support Section Technology Development Manager

The NSF Polar Research Support Section Technology Development Manager oversees the development and implementation of USAP Certification & Accreditation activities.

6.3 USAP Information Security Manager (ISM)

The USAP ISM implements the C&A program and coordinates its activities with other IT programs and organizations. The ISM ensures project plans and budgets include C&A activities as appropriate. The ISM directs the site C&A process. The ISM coordinates C&A activities with the NSF Information Security Officer, and with other USAP participating agencies. This includes planning the efforts, obtaining evaluation resources, and overseeing production of the C&A package. The ISM works closely with the designated C&A project lead to make recommendations to the USAP Certifying Official.

6.4 USAP Information Systems Owners and Developers

System owners and development managers will ensure their systems comply with this policy, with NSF certification & accreditation guidance, and with NIST instructions.

6.5 Non-USAP Information Systems Owners and Developers

System owners and development managers for Non-USAP systems will ensure their systems comply with this policy, with NSF certification & accreditation guidance, and with NIST instructions to the extent applicable for their systems.

7. CERTIFICATION & ACCREDITATION PROGRAM IMPLEMENTATION

The USAP Information Security Manager will develop appropriate policies, processes, and procedures to implement the USAP Certification & Accreditation Program. The USAP C&A program will identify security risks associated with operation of all applicable information systems to certify and accredit those systems for operation. USAP participant organizations will publish procedures as needed to comply with this policy.

7.1 Guiding Standards

The USAP C&A process will be based on existing federal and NSF directives.

7.2 Certification & Accreditation Organization and Administration

The USAP ISM will establish teams as needed to complete C&A activities. These teams will complete C&A activities for their assigned systems, and ensure documentation packages are completed. These teams will support the certification activities of all USAP participant organizations and Non-USAP systems owners, as directed by NSF OPP.

7.3 Policy Review

The USAP Information Security Program Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP

8. AUTHORITY

Publication of this policy is in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002 and NSF Manual 7, The NSF Information Security Handbook.

KARL A. ERB
Director